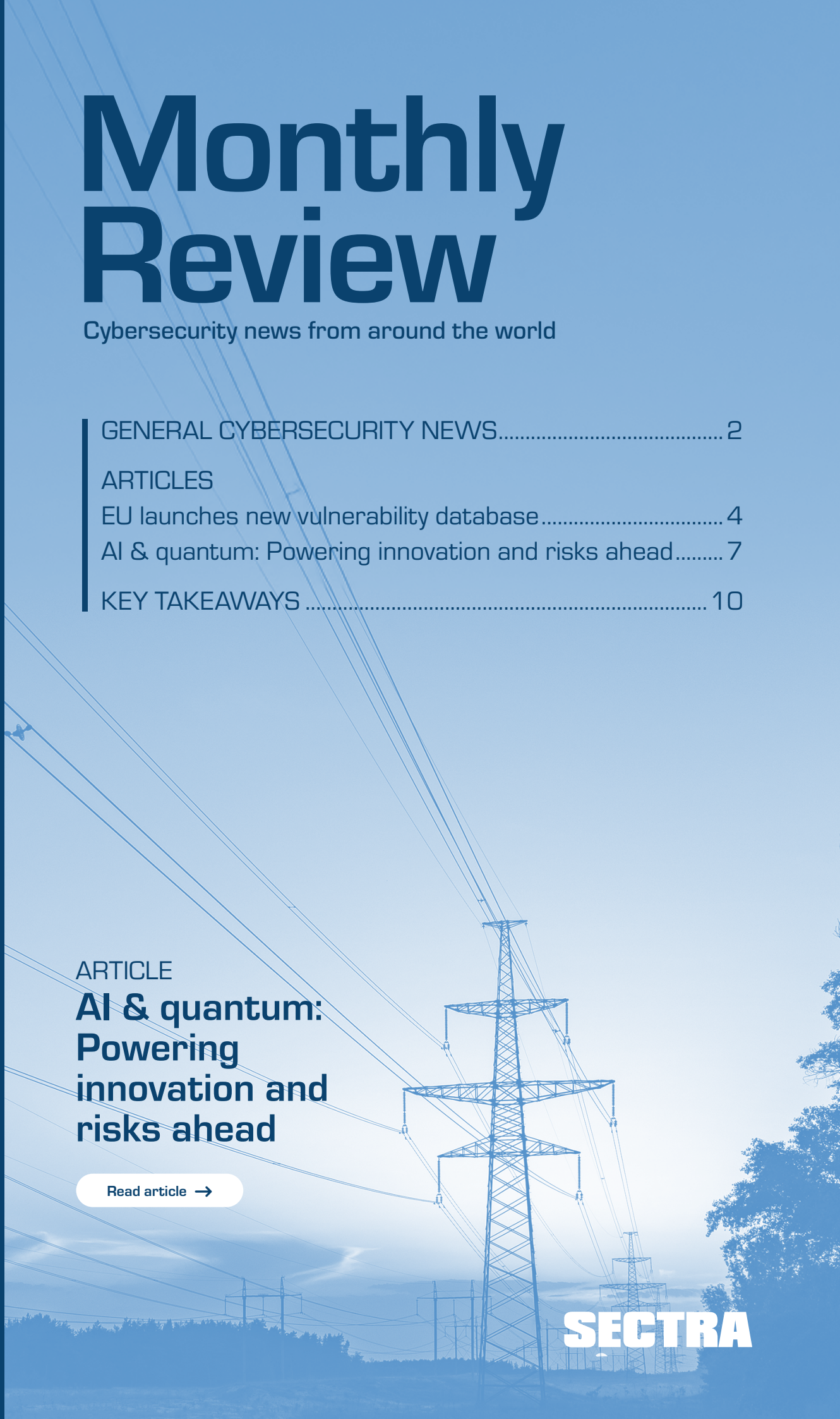
Monthly Review

Cybersecurity news from around the world



ARTICLE

AI & quantum: Powering innovation and risks ahead

Read article →

SECTRA

General cybersecurity news

1 Over 60 million affected—as power outage reveals risks

In late April, Spain and Portugal experienced a massive power outage affecting over 60 million people. Reuters reported the blackout began with a sudden loss of power generation in Granada, followed by disconnections in Badajoz and Seville, equivalent to the loss of two large nuclear plants and a collapse of the Iberian power system. Major cities like Madrid, Barcelona, and Lisbon were left without electricity for several hours, causing widespread disruptions.

Spanish authorities have ruled out a cyberattack as the cause. The Ministries of Energy and Interior stated there is no evidence of digital sabotage targeting grid operator REE, according to Reuters. Following the outage, authorities have initiated a review to assess whether small and medium-sized power producers, including renewables, may have been a weak link exploited in the incident. Spain's National Cybersecurity Institute (Incibe) stated the review also seeks to evaluate the overall cyber defenses of these producers.

Regardless of the cause, the incident highlights vulnerabilities in critical infrastructure and the need to strengthen security measures against risks, including cybersecurity. Ensuring resilience in energy systems requires a balance between technical reliability and proactive cyber defense. Investment in comprehensive security practices is crucial to minimize disruptions impacting vital services.

2 Three simple steps to protect your organization from cyber threats

Several EU and Swedish agencies report rising cyber threats against public and private organizations. Protecting critical societal functions and sensitive data requires essential security measures.

1. **Stay updated**: Always install the latest updates and security patches on all apps, operating systems, and hardware. This helps close security gaps before attackers exploit them.
2. **Backup your sensitive data**: Regularly back up important information to a secure place. Reliable backups ensure data recovery if lost or compromised.
3. **Redundancy**: Keep at least two copies of every critical system or component. If one fails, the other takes over immediately, minimizing downtime.

By implementing these security measures, your organization is better equipped to mitigate risks and respond effectively to potential attacks.

3 MSB: Cyberattacks threaten essential services

A biennial risk assessment from the Swedish Civil Contingencies Agency (MSB), released in late April, warns that sophisticated cyberattacks could disrupt critical systems across Sweden, affecting electricity, transport, healthcare, and payments. Malicious code could rapidly spread through supply chains and exploit unknown vulnerabilities.

The report outlines scenarios where core functions are paralyzed—flights canceled, surgeries postponed, food deliveries delayed. MSB notes many organizations lack basic cybersecurity practices, leaving them vulnerable even to low-complexity threats.

Cyber risks, according to the report, are now a direct threat to society's functions, disrupting healthcare, energy, and transport systems. The key question isn't *if* systems will be targeted—but whether we'll be ready when they are.

ARTICLE

EU launches new vulnerability database

One month after uncertainty around the CVE program's funding, the EU has launched the European Vulnerability Database (EUVD) under NIS2. This new platform aims to provide a unified source for vulnerability information in Europe.

In last month's newsletter, we covered the uncertain situation following MITRE's announcement that it would no longer fund the Common Vulnerabilities and Exposures (CVE) program—the backbone of global vulnerability management—which sent shockwaves through the cybersecurity community. Although the U.S. Cybersecurity and Infrastructure Security Agency (CISA) quickly stepped in to secure continued funding, the episode highlighted Europe's dependency on non-European systems to protect critical digital infrastructure.

Now, one month later, the European Union has taken a clear step toward addressing that dependency. On May 13, the European Union Agency for Cybersecurity (ENISA) announced the launch of the European Vulnerability Database (EUVD), a key element in the EU's cybersecurity framework under the NIS2 Directive. The EUVD serves as a centralized platform for collecting and sharing information about vulnerabilities affecting IT products and services across Europe.

"The EUVD is a significant advancement in enhancing Europe's cybersecurity resilience and autonomy", said Henna Virkkunen, European Commission Executive Vice-President for Tech Sovereignty, Security, and Democracy. →

For the first time, Europe has a unified platform aggregating detailed information on known vulnerabilities—including risk assessments, exploitation status, affected products, and mitigation advice. The data comes from multiple sources, such as MITRE's CVE catalog, CISA's Known Exploited Vulnerability (KEV) list, national CSIRTs, and vendor alerts.

While the EUVD increases European digital sovereignty, it is not meant to replace the CVE program but to complement and build upon it. Since January 2024, ENISA has operated as a CVE Numbering Authority (CNA), enabling it to register vulnerabilities identified by EU CSIRTs or reported within the EU. This participation allows Europe to contribute directly to the global vulnerability ecosystem while maintaining control over its own data management and sharing.

"Europe no longer aims to simply react to vulnerabilities; it aims to take control"

"The database is an essential tool for improving vulnerability and risk management", said Juhan Lepassaar, ENISA's Executive Director. "It provides increased transparency and better decision-making resources for all users of affected ICT products".

EUVD is publicly accessible and designed for a broad range of users, including suppliers, end-users, national authorities, and security researchers. The platform offers three main dashboards highlighting critical vulnerabilities, actively exploited vulnerabilities, and EU-coordinated vulnerabilities managed collaboratively by the European CSIRT network.

By combining open-source data, national advisories, vendor patch information, and exploitation status, the EUVD provides a reliable and actionable resource for proactive cybersecurity. →

With the upcoming Cyber Resilience Act requiring manufacturers from September 2026 to report exploited vulnerabilities through the Single Reporting Platform (SRP), the EUVD remains an informational and analytical platform focusing on transparency and shared risk management based on publicly available data.

Throughout 2025, ENISA will continue to develop the EUVD, incorporating user feedback to improve its functionality. The goal is for the EUVD to become an indispensable tool for public and private sector actors as well as security researchers—demonstrating how European cybersecurity strategies can translate into practical measures.

At a time when cybersecurity threats are global but political decisions increasingly localized, the launch of the EUVD signals a shift in Europe's approach. Europe no longer aims to simply react to vulnerabilities; it aims to take control. By strengthening its vulnerability management ecosystem, the EU is laying the foundation for greater resilience, quicker response, and enhanced digital sovereignty. ■

ARTICLE

AI & quantum: Powering innovation and risks ahead

As AI and quantum technologies evolve, they promise innovation while reshaping cybersecurity and global stability. Reports by both NATO and CrowdStrike explore their transformative potential—as well as the risks they pose.

NATO's Science and Technology Organization (STO) report *Macro Trends 2025–2045*, highlights that nations with expertise in artificial intelligence (AI) and quantum technologies will gain strategic advantages in addressing future challenges. The report explains how these technologies could transform sectors such as defense, healthcare, and energy by predicting cyber threats, optimizing resources, and tackling global challenges—like climate change and vulnerabilities in critical infrastructure.

AI's ability to analyze large datasets and detect patterns is already a key component of cybersecurity systems. NATO points out that AI helps identify cyber threats early by analyzing anomalies in network traffic and predicting attack patterns. Combined with quantum technology, security systems gain additional strength through innovations such as quantum encryption, which protects data communications from advanced threats. The report also emphasizes the importance of securing vulnerable critical systems, including energy grids. →

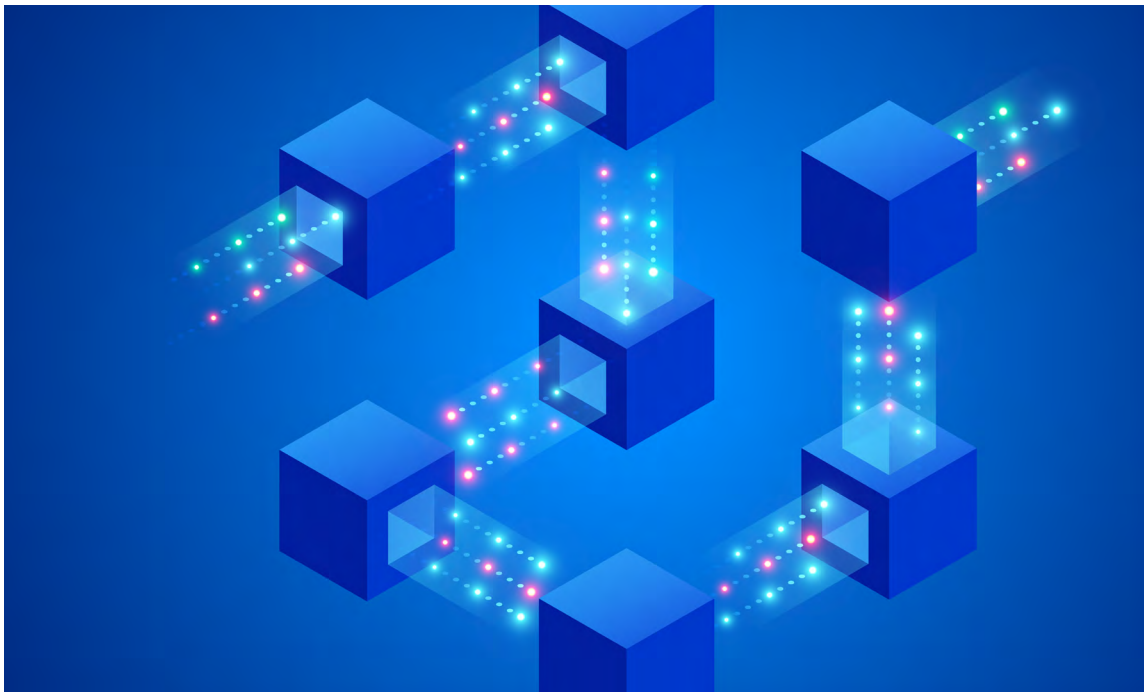
Although quantum technology is still developing, it promises major innovations. STO expects quantum computers to be widely adopted by 2029, breaking traditional encryption algorithms and enabling new protections such as quantum key distribution (QKD). Quantum sensors that detect changes in movement and gravity with extreme accuracy can improve navigation without GPS, useful in military contexts like submarine navigation and civilian uses such as autonomous vehicles.

However, challenges remain, including high energy consumption and dependence on materials like gallium and germanium. The report highlights bioengineered materials and green energy technologies as vital for driving these innovations.

"AI and quantum technologies both drive innovation and pose risks to economic and geopolitical stability"

The United States and China lead the global race for technological dominance. In 2021, the U.S. spent approximately $806 billion on research and development (3.48% of GDP), while China spent $668 billion (2.43% of GDP). China's investments in technology education are expected to produce twice as many STEM PhDs as the U.S. by 2025. According to the NATO-report, these efforts enhance their capabilities to combat cyber threats and develop energy solutions for climate-related challenges.

CrowdStrike, the U.S.-based cybersecurity company specializing in threat detection and IT system protection, offers insights through its *Global Threat Report 2025*, providing a complementary perspective by focusing on how AI is increasingly used by cybercriminals. →



CrowdStrike says that generative AI (GenAI) is exploited to create malware and conduct sophisticated cyberattacks. For example, in March 2024, Snake Keylogger malware was distributed through spam emails containing AI-generated text. Snake Keylogger logs keystrokes and steals sensitive information such as passwords—enabling attackers to access accounts and systems. CrowdStrike also notes that AI-generated fake websites and AI-automated ransomware coding make cyberattacks more effective and harder to detect.

Both of the reports demonstrate that AI and quantum technologies both drive innovation and pose risks to economic and geopolitical stability. Strategic investments in research, energy solutions, and cybersecurity are necessary to realize their potential while mitigating risks. Long-term planning and international cooperation will be crucial for balancing technological advancements with effective safeguards, shaping the future of security and innovation. ■

Key takeaways

1. Spain's blackout exposed critical infrastructure risks; cyberattack ruled out, but security reviews are underway.

2. Three simple steps to protect your organization: update systems, back up data, and ensure redundancy.

3. MSB warns cyberattacks threaten essential services—basic cybersecurity and readiness are crucial.

4. The EU launches the European Vulnerability Database (EUVD) to boost digital sovereignty and vulnerability management.

5. AI and quantum tech fuel innovation but raise cybersecurity risks—strategic investment and cooperation needed.

www.communications.sectra.com
communications@sectra.com

Sectra Communications is headquartered in Linköping, Sweden,
and operates through offices in Sweden, the Netherlands and Finland.

Linkedin

SECTRA